Accellion

The world's simplest large file transfer solution.™

Content Monitoring & Filtering Module for Data Leak Prevention

Extends Accellion file transfer to enable policy-based content-aware data leak prevention for data-in-motion.

The Accellion DLP Module for Content Monitoring and Filtering addresses the increasing need to secure and control the movement of sensitive enterprise data to protect intellectual property and ensure compliance. The Accellion Content Monitoring and Filtering module enables organizations to not only secure the transfer of files but also for the first time be able to monitor, and analyze the content of file transfers, and filter file transfers based on corporate policy, for protection of IP and compliance requirements.

Securing Data-in-Motion

An important element of any enterprise strategy for data leak prevention is ensuring security and compliance for data-in-motion. Many organizations have invested in email security and encryption technologies however with 10MB limits of email attachments the lion share of data-in-motion is moving over unsecured, unmonitored channels. File transfer needs to be a major consideration in moving enterprise data. Accellion extends its managed file transfer solution with content monitoring and filtering to ensure that file transfer is not only secure and tracked but also is monitored and filtered based on policy-based content-awareness.

Avoiding Data Breaches

No company wants to experience a data breach. Data breaches make headline news and have serious financial consequences.

Corporations and government agencies need to demonstrate that they are controlling sensitive information. SOX, HIPAA, GLBA, FDA regulations require auditable records of all data transfers to demonstrate compliance.

No company wants to fail a security audit. Yet if file transfer security is not addressed – it will be flagged. Un-secure, un-monitored, and un-filtered file transfer is a data breach waiting to happen.

Important Security Questions

How can I share information?

- How can I send files too big for email?
- Is it okay for me to transfer information on a thumb drive?
- Is P2P file sharing safe for corporate use?
- Is IM suitable for employees to transfer digital information?

What information can I share and with whom?

- Who decides what files can be shared and with whom?
- What information is considered valuable intellectual property?
- What information is controlled by compliance regulations?

Who is responsible for protecting sensitive information?

- What controls are in place to safeguard employees?

Best-of-Breed Technologies

The Accellion content monitoring and filtering module for DLP is designed to integrate with commercially available Data Leak Prevention solutions via the industry standard ICAP protocol.

Impact of Data Leakage

- Compliance violations
- Loss of competitive advantage
- Negative branding
- Financial consequences
- Customer trust

KEY BENEFITS

- Extends Accellion file transfer to enable policy based content-aware data leak prevention.
- Provides additional security protection for intellectual property and sensitive information subject to industry and government compliance regulations.
- Monitors and filters Accellion file transfers according to corporate data protection policies.
- Enables integration of Accellion managed file transfer with industry leading data leak prevention solutions.

Enhanced Data Protection

An enterprise strategy for data leak prevention must consider data-in-motion. The Accellion DLP Module for Content Monitoring and Filtering enhances file transfer data protection. Files sent via Accellion are not only securely transferred and tracked but also file content can be inspected against corporate security policies and either quarantined or blocked.

Enhanced Data Security

The Accellion DLP Module for Content Monitoring and Filtering extends Accellion Managed File Transfer security features.

File/Data Security

For each transferred document, the Accellion Appliance provides a secure link generated by a double 128-bit MD5 token. SSL/TLS is used for encrypting file uploads and downloads using HTTPS. IPSec is used as files are replicated between appliances.

Business Level Security

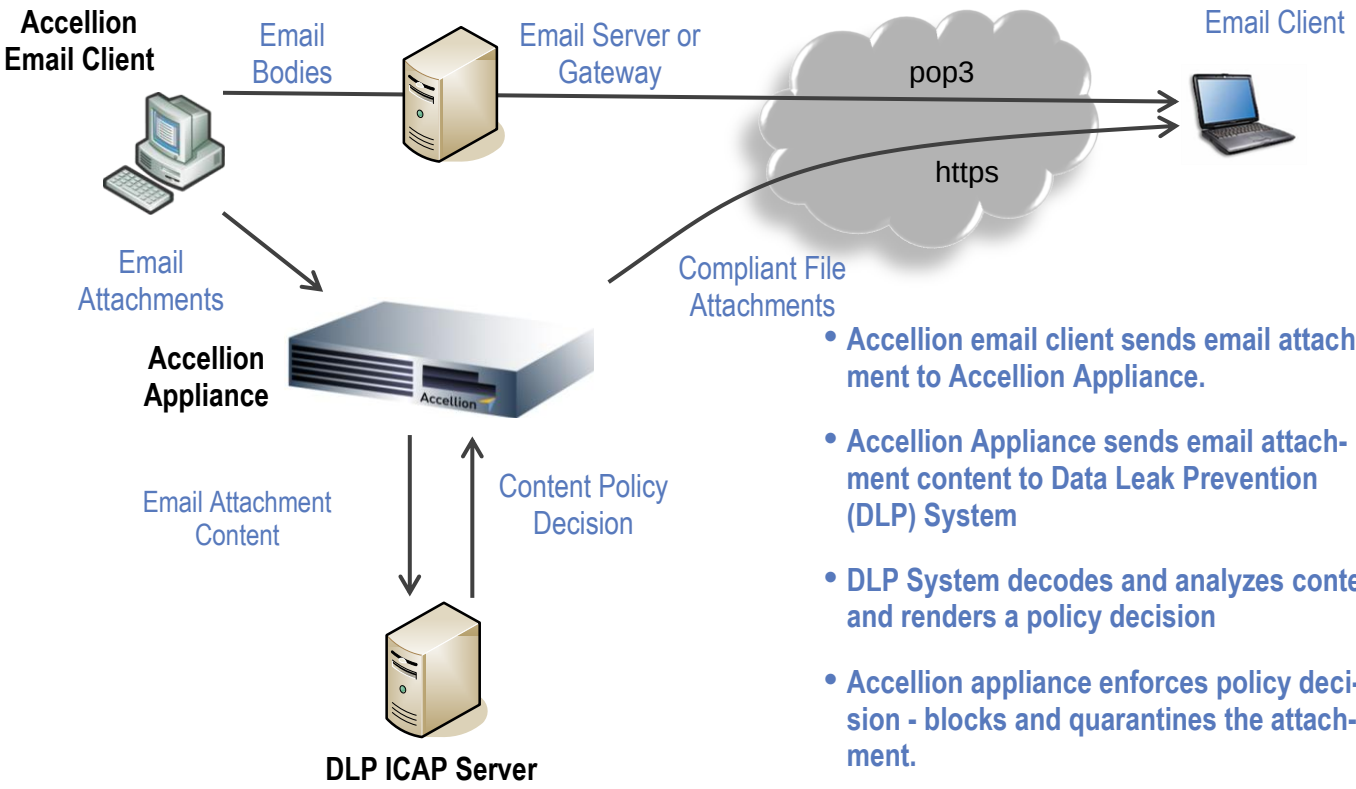
Accellion file transfer contains an authentication check point to validate recipients so confidential information is not overexposed. Users get return receipts with every file transfer and Accellion provides an audit trail with its file tracking.

Policy-based Content-Aware DLP

All files are subject to deep content inspection. Once inspected the Accellion Content Monitoring and Filtering Module either transfers the file or quarantines or blocks based on content inspection results.

KEY FEATURES

- Integrated file content monitoring and filtering for data leak prevention.
- Best-of-breed managed file transfer combined with best-of-breed DLP.
- Blocks and quarantines file transfers that violate corporate policy.
- Integration with DLP systems via industry standard ICAP protocol.
- Encryption via SSL
- LDAP/AD Integration
- Comprehensive file tracking and reporting
- Audit Trail



- **Accellion email client sends email attachment to Accellion Appliance.**
- **Accellion Appliance sends email attachment content to Data Leak Prevention (DLP) System**
- **DLP System decodes and analyzes content and renders a policy decision**
- **Accellion appliance enforces policy decision - blocks and quarantines the attachment.**

Accellion, Inc.
1900 Embarcadero Road
Suite 207
Palo Alto, CA 94303

Tel +1 650 739-0095
Fax +1 650 739-0561
www.accellion.com
info@accellion.com